# Fiche Technique de mise en place d’un SSO

## Qu’est que le SSO

Le SSO (Single Sign On) est une procédure d’authentification consistant à acceder à plusieurs applications à partir d’une connexion unique. C’est-à-dire qu’à partir d’une connexion avec un compte IdP, l’utilisateur a accès à plusieurs applications sans avoir besoin de s’authentifier à chaque utilisation d’une nouvelle application.

## Avantages du SSO

Le SSO présente de nombreux avantages tels que :

* Productivité : avec l’utilisation du SSO les entreprises gagneront en temps dans l’utilisation de leurs diverses applications ;
* Un seul compte peut avoir accès à plusieurs ressources ;
* Flexibilité dans la gestion des comptes : le SSO permet également d’attribuer les accès aux utilisateurs à différentes applications.

## Comment mettre en place un SSO

### Choisir un protocole SSO

Ici, il est question de définir comment les données authentifiées et autorisées sont échangées entre les applications web et le fournisseur d’identité. Dans cette partie nous avons à faire le choix entre 2 protocoles et chaque protocole ayant sa spécificité :

1. OpenID Connect (OIDC)

Protocole d’identité qui utilise les mécanismes d’autorisation et d’authentification 0Auth2.0 (protocole permettant d’avoir accès à un site web ou une application à des ressources protégées de l’utilisateur) servant à vérifier l’identité d’un utilisateur d’un service client. Il utilise 0Auth2 comme protocole sous-jacent. Ses spécificités sont les suivantes :

* Il utilise le JWT (JSON Web Token), c’est-à-dire que lors de la l’authentification d’un utilisateur il lui est attribué un bail (token) pour une durée déterminée d’utilisation de l’application ;
* Le flux de données en HTTP (HypperText Transfer Protocol) ;
* Evite de partager les informations d’identification de l’utilisateur avec les services.

1. SAML (Security Assertion Markup Language)

C’est un protocole d’authentification utilisant le format XML pour les échanges des données entre deux fournisseurs de services. Les utilisateurs se connectent sans avoir à transmettre les données sur le web. Lorsque créée une connexion, les informations relatives à l’utilisateur ne dépendent ni de l’endroit, ni de l’adresse IP.

Il utilise un protocole de Mapping définissant les messages de requête et de réponse pour la communication entre deux fournisseurs de services. Parmi ces protocoles de communication nous avons :

* Reverse SOAP Binding : pour la définition des messages SAML dans un environnement SOAP)
* HTTP Post Binding : pour la définition des messages via la procédure http
* http Artifact Binding
* SAML URI (Uniform Ressource Identifier) Binding

### Configurer le IdP et les applications web

Cette partie consiste configureer l’idP et les applications web pour activer le SSO. Cela implique de nombreuses configuration telles que : des points de terminaisons, paramètres, certificats et métadonnées nécessaires à la communication et vérification des demandes et réponses SSO.

### Tester et debugger l’implémentation

Tester les fonctionnalités SSO sur différentes perspectives telles que le login utilisateur, logout, gestion des sessions, gestion des erreurs et la vérification d’identité. Contrôler chaque potentielles vulnérabilités.

### Former les utilisateurs des applications web

Former sur comment utiliser le SSO, les avantages et risques de celuici.

### Eduquer et former les developpeurs de l’application web

Former sur comment implémenter et maintenir un SSO, les meilleures pratiques et standard à suivre.

### Superviser et mettre à jour l’implémentation SSO

S’assurer que le SSO respecte les fonctionnalités, la sécurité et l’efficience. Superviser l’activité SSO, la performance régulière.